Specifying BYOD Policies With Authorisation Logic

Joseph Hallett and David Aspinall

THE UNIVERSITY *of* EDINBURGH
informatics

Corporate BYOD Policies

Employees bring their devices to work.

Companies find this challenging.

Policies are hard to follow

Employees must agree to follow corporate policies.

Policies are poorly specified.

Formal languages can help

Formal languages give us a framework for talking about policies rigorously.

Formal languages can help identify problems.

Employees bring their devices to work

81%

…of companies have some form of BYOD scheme or will do soon

- 40% have BYOD available to all employees
- 32% have BYOD available to select ones
- 9% plan to support it in the next year

BYOD & Mobile Security 2016 Spotlight Report. LinkedIn Information Security

Companies find this challenging

They don’t directly control the devices running on their networks

Mobile Device Management software is unsophisticated and unpopular

- Almost 50% of companies can’t even enforce their own policies
  Q4 Mobile Security and Risk Review. MobileIron.

MDM software is fairly basic

Mobile Device Management

Fairly basic at the minute

Limited to device provisioning, black and white listing apps, and requiring certain features to be turned on and off

Some more advanced schemes use *app wrapping*

- Modifies apps to use company controlled APIs
- Can be circumvented by installing non-modified apps, native code
- Breaks Android trust model

Android for Work

Google's method for keeping work apps separate from personal apps

- Have multiple instances of all your apps on your phone
- Mark the ones for work with a little sticker
- Use Android sandboxing mechanisms to enforce separation

Designed to help prevent mixing of personal and work data, not really enforce corporate policies

- Work apps can't access your photos
- Personal apps can't access your spreadsheets

Employees must agree to follow policies

Natural language policies which describe in high level terms what is allowed on BYOD devices

Most are extremely simple but they’re becoming more sophisticated

- Most say turn on encryption, and don’t install dodgy apps
- SANS publish guidelines for companies writing them
- CESG offer advice and guidance

Problem:

Policies are imprecise and hard to reason about and compare

How do we know if a policy has problems?

How could we start to enforce complex policies automatically?

AppPAL:

Instantiation of the SecPAL authorisation logic for saying what apps you want

When applied to BYOD we can use it to think about and enforce policies

We can use it to find potential problems in natural language polices

Translating Policies into AppPAL

AppPAL is designed to be readable

We present excerpts from the AppPAL translation of 3 BYOD policies

- *Security Policy for the use of handheld devices in corporate environments. SANS*
- *Mobile Devices Policy. Torbay and Southern Devon Health Care NHS Trust*
- *Use of Personally Owned Devices for University Work. University of Edinburgh*

What apps can you install?

SANS: *"The IT Department maintains a list of allowed and unauthorised applications and makes them available to users on the intranet."*

```
'sans-policy' says
  'it-department' can-say
    App isInstallable.
```

Edinburgh: *"Only download applications (apps) or other software from reputable sources."*

```
'edinburgh-policy' says
  Store can-say App
isInstallable
  if Store sells(App),
     Store isReputable.
```

Policies are problematic

SANS: *“The IT Department maintains a list of allowed and unauthorised applications and makes them available to users on the intranet.”*

```
'sans-policy' says
  'it-department' can-say
    App isInstallable.
```

Policies are problematic

SANS: *“Only approved third party applications can be installed on handhelds. The approved list can be obtained by contacting the IT department, or should be available on the intranet.”*

```
'sans-policy' says
  'it-department' can-say
    App isInstallable.
```

Policies are problematic

NHS: *"Apps for work usage must not be downloaded onto corporately issued mobile devices (even if approved on the NHS apps store) unless they have been approved through the following Trust channels: Clinical apps; at the time of writing there are no apps clinically approved by the Trust for use with patients/clients. However, if a member of staff believes that there are clinical apps* [...] *ratification should be sought via the Care and Clinical Policies Group.* [...] *Business apps; at the time of writing there are no business (i.e., non-clinical) apps approved by the Trust for use other than those preloaded onto the device at the point of issue. However, if a member of staff believes that there are apps* [...] *ratification of the app must be sought via the Management of Information Group (MIG).* [...] *Following approval through Care and Clinical Policies and/or MIG, final approval will be required through Integrated Governance Committee."*

Policies are problematic

```
'nhs-policy' says App isInstallable
  if App isUsable,
     App isFinallyApproved.

'nhs-policy' says 'cacpg' can-say App isUsable
  if App isUsableClinically.

'nhs-policy' says 'mig' can-say App isUsable
  if App isUsableNonClinically.

'nhs-policy' says 'igc' can-say App isFinallyApproved.
```

Policies are problematic

NHS: *"Apps for work usage must not be downloaded onto corporately issued mobile devices (even if approved on the NHS apps store) unless they have been approved through the following Trust channels: Clinical apps; at the time of writing there are no apps clinically approved by the Trust for use with patients/clients. However, if a member of staff believes that there are clinical apps* [...] *ratification should be sought via the Care and Clinical Policies Group.* [...] *Business apps; at the time of writing there are no business (i.e., non-clinical) apps approved by the Trust for use other than those preloaded onto the device at the point of issue. However, if a member of staff believes that there are apps* [...] *ratification of the app must be sought via the Management of Information Group (MIG).* [...] *Following approval through Care and Clinical Policies and/or MIG, final approval will be required through Integrated Governance Committee."*

Policies are problematic

```
'nhs-policy' says App isInstallable
  if App isUsable,
     App isFinallyApproved.

'nhs-policy' says 'cacpg' can-say App isUsable
  if App isUsableClinically.

'nhs-policy' says 'mig' can-say App isUsable
  if App isUsableNonClinically.

'nhs-policy' says 'igc' can-say App isFinallyApproved.
```

AppPAL can help

```
The following assertions are unsatisfiable:
  'nhs-policy' says App.1 isInstallable if App.1 isUsable, App.1
isFinallyApproved.


These decisions may be derivable but we lack statements from the
delegated party:
  (via 'mig')   'nhs-policy' says * isUsable
  (via 'igc')   'nhs-policy' says * isFinallyApproved
  (via 'cacpg') 'nhs-policy' says * isUsable
```

A common language of BYOD policies

SANS: *"Conducting telephone calls or utilizing handhelds while driving can be a safety hazard. Drivers should use handhelds in hand only while parked or out of the vehicle. If employees must use a handheld device while driving, Company requires the use of hands-free headset devices."*

NHS: *"For safety reasons, Trust staff must not use a hand held mobile device whilst driving any vehicle.* […] *the Trust does not recommend using mobile devices in hands-free mode* […] *whilst driving. "*

A common language of BYOD policies

```
'sans-policy' says
  Device mustNotOperate
  if
    Device isOwnedBy(Owner)
  where
    inCar(Device) = true,
    isDriving(Owner) = true,
    isHandsFree(Device) = false.
```

```
'nhs-policy' says
  Device mustNotOperate
  if
    Device isOwnedBy(Owner)
  where
    inCar(Device) = true,
    isDriving(Owner) = true.
```

A common language of BYOD policies

Edinburgh: *"Control your devices connections by disabling automatic connection to open, unsecured Wi-Fi networks."*

SANS: *"If mobile workers do require connectivity through public, open, or untrusted WLAN, then users MUST use WLANs using, if available and in this order: WPA(2) encryption, WEP 256 bits (or 128 bits), or finally open networks if nothing else is available. Users connected to data networks in an open environment MUST use a VPN connection."*

A common language of BYOD policies

```
'edinburgh-policy' says
  Device canConnectTo(AP)
  if AP isSecure.
```

```
'sans-policy' says
  Device canConnectTo(AP)
  if AP isSecure.
```

```
'sans-policy' says
  Device canConnectTo(AP)
  if Device hasVPN(VPN)
  where connect(VPN) = true.
```

```
'sans-policy' says AP isSecure if AP canUseWPA2.
'sans-policy' says AP isSecure if AP canUseWEP256.
'sans-policy' says AP isSecure if AP canUseWEP128.
```

Evidence with AppPAL

NHS: *"Some mobile devices have the ability to take photographs/videos. This function should not be used for photographs/videos of an individuals care and treatment unless the device has encryption enabled and it is clinically appropriate to do so. If the photography/video facility is used as part of the recording of an individuals care and treatment, the device user must ensure that the consent of the* individual *has been collected prior to taking any photograph/video.* [· · ·] *A record of the consent must be entered into the individuals care record."*

Evidence with AppPAL

```
'nhs-policy' says Device canPhotograph(Patient)
  if Device isEncrypted, Patient canBePhotographed.

'nhs-policy' says 'clinician' can-say Patient canBePhotographed
  if Patient hasClinicalNeedForPhotograph,
     Patient hasConsentedToPhotograph
  where recordedICRConsentForPhotograph(Patient) = true.

'nhs-policy' says  'clinician' can-say
  Patient hasClinicalNeedForPhotograph.

'nhs-policy' says Patient can-say
  Patient hasConsentedToPhotograph
  if Patient canConsent.
```

To review…

Brief taste of what we can do with AppPAL

Shown some examples from BYOD policies and how they can be formalized

To review…

BYOD policies at present are very simple but they're getting more advanced and with more complex relationships

Existing MDM tools are (relatively) primitive and underwhelming

Scope for formal methods to help

- Enforcing policies
- As a framework for thinking about policies

Questions?

Joseph Hallett
J.Hallett@sms.ed.ac.uk

https://github.com/apppal/libapppal